UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,344	07/22/2003	Jeffrey S. Bardsley	5577-265	7591

20792 7590 07/25/2007

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/624,344	BARDSLEY ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/30/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 4/11/2007, PROSECUTION IS HEREBY REOPENED. The new grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Gilberto Barron.

2. Claims **1-23** have been examined.

Information Disclosure Statement PTO-1449

3. Information disclosure statements submitted by applicant dated 3/30/2007 was considered. Please see attachment PTO-1449.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 18-23 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed invention does not fall within at least one of the four categories of patent eligible subject matter (process, machine, manufacture, or composition of matter). The claimed invention is a data structure, which is neither a method nor produces a tangible embodiment.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 1-23 rejected under 35 U.S.C. 103(a) as being unpatentable over Friedrichs et al. (U.S. Patent Application Publication No. 2003/0084349 A1, filed August 9, 2002), and further in view of Gupta et al. (U.S. Patent Application Publication No. 2003/0004689 A1, filed June 13, 2002).

7.1. As per claim 1, Friedrichs and Gupta are directed to a method of generating computer security threat management information (Friedrich paragraph 8-10), comprising: receiving notification of a computer security threat (Friedrich paragraph 40 to 44 or 20-30); generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received (as described in Friedrich paragraphs 17-20, security event data is collected from all network devices, and stored in fields of a database. The Extractor 120 performs analysis on data and stores the analysis result in the upload server or the database server (parag. 20). In addition, Friedrich paragraphs 30-45 teach database server 230 supplementing demographic and geographic information regarding the network generating the security events (parag. 30 and 35), identifying and storing validated security threats based on security event data (parag. 37), the All Events database, which includes all security events (parag. 40-41) and Product database 450, which includes information about specific products that exhibit vulnerabilities, product version information, and details about how to patch a flaw, or other security measures

that a network operator could implement, and how to repair a damage (parag. 45). All the mentioned data and databases are combined in a single database such as Threat database (parag. 46). Therefore, the Threat database contains a set of fields related to a security threat and its associated data.), the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (per Friedrich paragraph 42, information stored in databases and included in the analysis and report includes demographic data. Per paragraph 35, the demographic data includes type of network and Operating System), a second computer-readable field that provides identification of a release level for the system type (per Friedrich paragraph 42, the proprietary information of security devices are included in the databases for analysis and report, in addition to demographic information, which shows detailed specifications of systems involved in the security threat are completely collected in the databases. Also note that the version information of the products is stored in Product database (Friedrich parag. 45)), and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (Friedrich paragraph 45);

As discussed above, Friedrichs teaches creation of a database including relevant information for detection and mitigation of attacks. Friedrich also teaches reporting the data for analysis, for example, by network administrators, but it does not explicitly teach transmitting the computer-actionable TMV (a data structure, such as a file) that is

generated to a plurality of target systems for processing by the plurality of target systems.

Gupta is directed to a system for provisioning computers against computer attacks, which includes, constructing a hierarchy of attacks and countermeasures, identifying attacks and associated detection and protection measures, and downloading the detection and protection measures to the target platform (Abstract). As indicated in Fig. 15- 17, and paragraphs 164 to 165, a data structure containing all information such as what attacks a given environment is vulnerable to, what protection means are available, and how detection alerts are correlated is created. The detection and protection measures are put in an attack file, and downloaded to the target systems for detecting and mitigating attacks. Therefore, Gupta teaches creation of a data structure, such as a file, that can be downloaded to the systems to be protected (target systems), such that the target system would mitigate the attacks based on the downloaded file.

Gupta and Friedrichs are clearly directed to analogous arts. At the time of invention, it would have been obvious to the one skilled in art to use Friedrich's system, which collects; generates, and store threat management information in a data structure, and modify it, according to Gupta's teachings, to create an attack file including the threat management information and the mitigation information, and send the attack file to target systems to mitigate the attacks associated with the threats.

The motivation for combination is creating a system that gathers all required information to create effective countermeasures, and deploys the created countermeasures to mitigate attacks. Friedrich paragraph 5-7 indicates the purpose of tying together information gathered from different devices, and aggregating information about network traffic, analyzing it to identify treats, and distributing it to neutralize the attack. Gupta paragraph 7-9 motivates and creates a single platform that gathers and uses all relevant data to produce provisioning data (attack file), which is downloaded to target systems to effectively mitigate attacks.

7.2. As per claim 2, Friedrichs is directed to a method according to claim 1 wherein the generating comprises selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format (Friedrich paragraphs 40-45, and paragraph 46 showing all mentioned databases could be combined to one database).

7.3. As per claim 3, Friedrichs is directed to a method according to claim 1 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level (Friedrich paragraph 35, 45, and 42).

7.4. As per claim 4, Friedrichs is directed to a method according to claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure

mode of installation (Friedrich paragraph 45 teaches including details about how to patch a flaw and security measures to mitigate a flaw. Examiner takes the official notice that installation mode (binary, manual, URL, local or server) is one of the details necessary to know when installing a patch, and therefore would have been obvious to the one skilled in art).

7.5. As per claim 5, Friedrichs is directed to a method according to claim 1 wherein at least one of the identifications comprises a pointer (Examiner takes the official notice that pointers are broadly used in databases to identify data. Therefore, it would have been obvious to use a pointer for identification of data).

7.6. As per claim 6, Friedrichs is directed to a method according to claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level (per paragraph 22, the Security Device 110 gathers details of elements participating in the threat. The details include ports, which is a subsystem if a network element. In addition, Hunter server 140 gathers further details such as IP address of system. As described in response to claim 1, the version level of subsystems are also collected and reported as

the comprehensive data about systems participating in the threat are recorded and reported).

7.7. As per claim 7, Friedrichs is directed to a method according to claim 6 wherein the subsystem type comprises an application program type (paragraph 35).

7.8. As per claim 8, Friedrichs is directed to a method according to claim 1 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat (per paragraph 43, Vendor signature databases contain a listing of all known security event types for a particular vendor, and therefore identifies the threats).

7.9. Limitations of claims 9 and 10 are substantially the same as claim 1 above.

7.10. As per claim 11, Friedrichs is directed to a system according to claim 9 further comprising a common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format (Fig. 4 and associated text), wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat (generation of a report based on user defined parameters was a well-known feature of database management systems at the time of invention).

7.11. Claims 12 to 23 are substantially the same as claims 1-8 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100